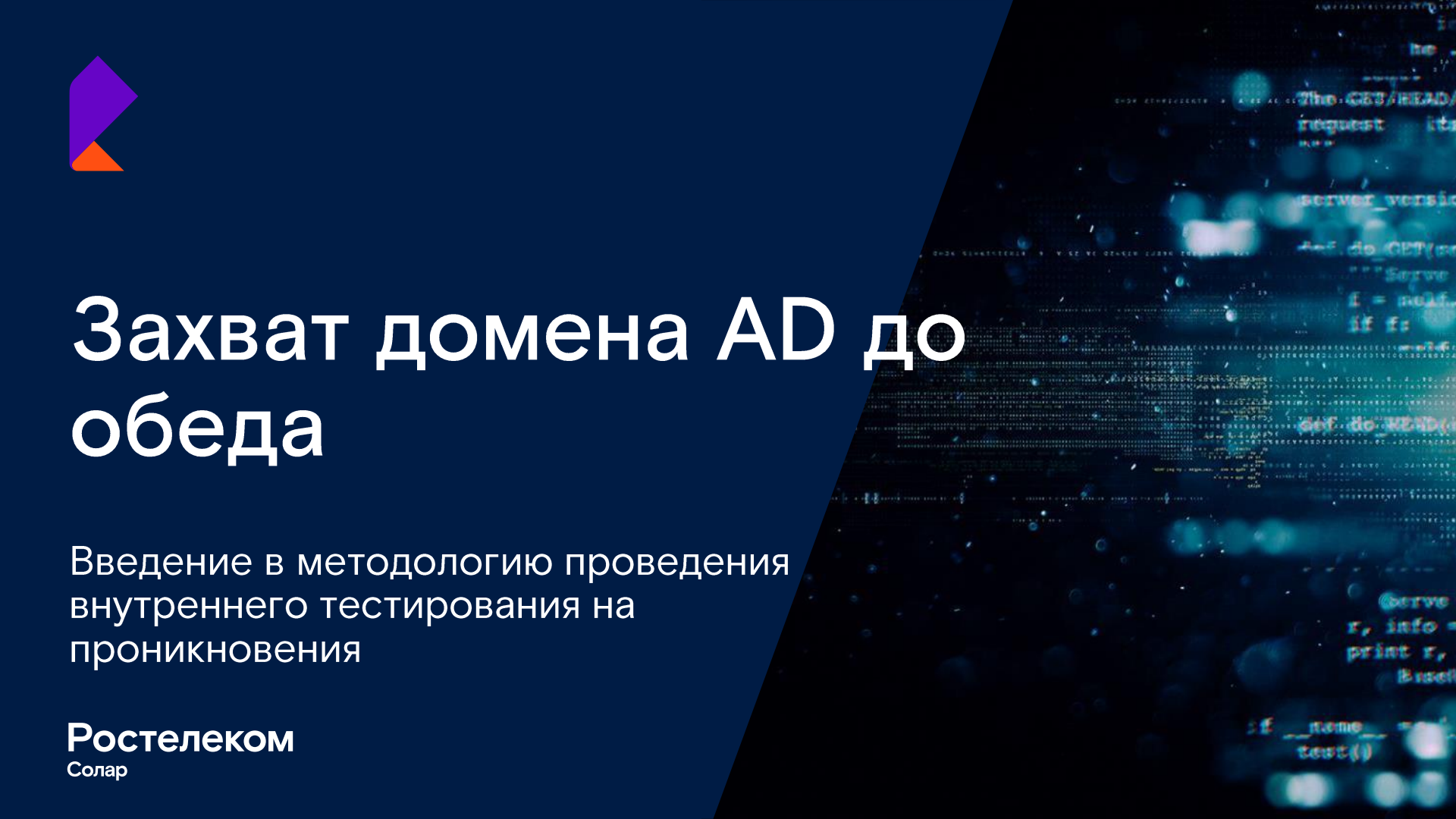


Захват домена AD до обеда

Введение в методологию проведения внутреннего тестирования на проникновения

Ростелеком
Солар

План

- Введение
- Классический метод тестирования на проникновение и его недостатки
- Первоначальные шаги
- Часто встречающиеся недостатки
- Вопросы

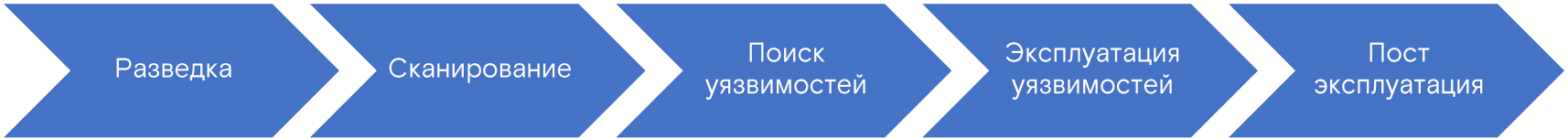
Несколько замечаний

- Не существует единственной правильной методологии проведения внутреннего тестирования на проникновения
- Внутреннее тестирование на проникновение != Red Teaming
  - Red Team – люди и процессы
  - Тестирование на проникновение – уязвимости и недостатки
- Получение привилегий Domain Admins не является конечной целью
- Два метода начального доступа
  - С доменной учетной записью
  - Без учетной записи (сетевой доступ)

Почему важно проводить внутренний пентест

- Тестирование на проникновение – проактивная защита
- Получение доступа во внутреннюю инфраструктуру вопрос времени, мотивации, опыта и удачи
  - Уязвимости в ПО (0-day) и веб приложениях
  - Социальная инженерия
  - Атака через подрядчика
- Прямой доступ серверов из сети Интернет во внутреннюю сеть, отсутствие DMZ.
- Средний промежуток времени от получения злоумышленниками доступа до их обнаружения от 120 дней
- Срок получения привилегий доменного администратора от 30 минут до 3 дней

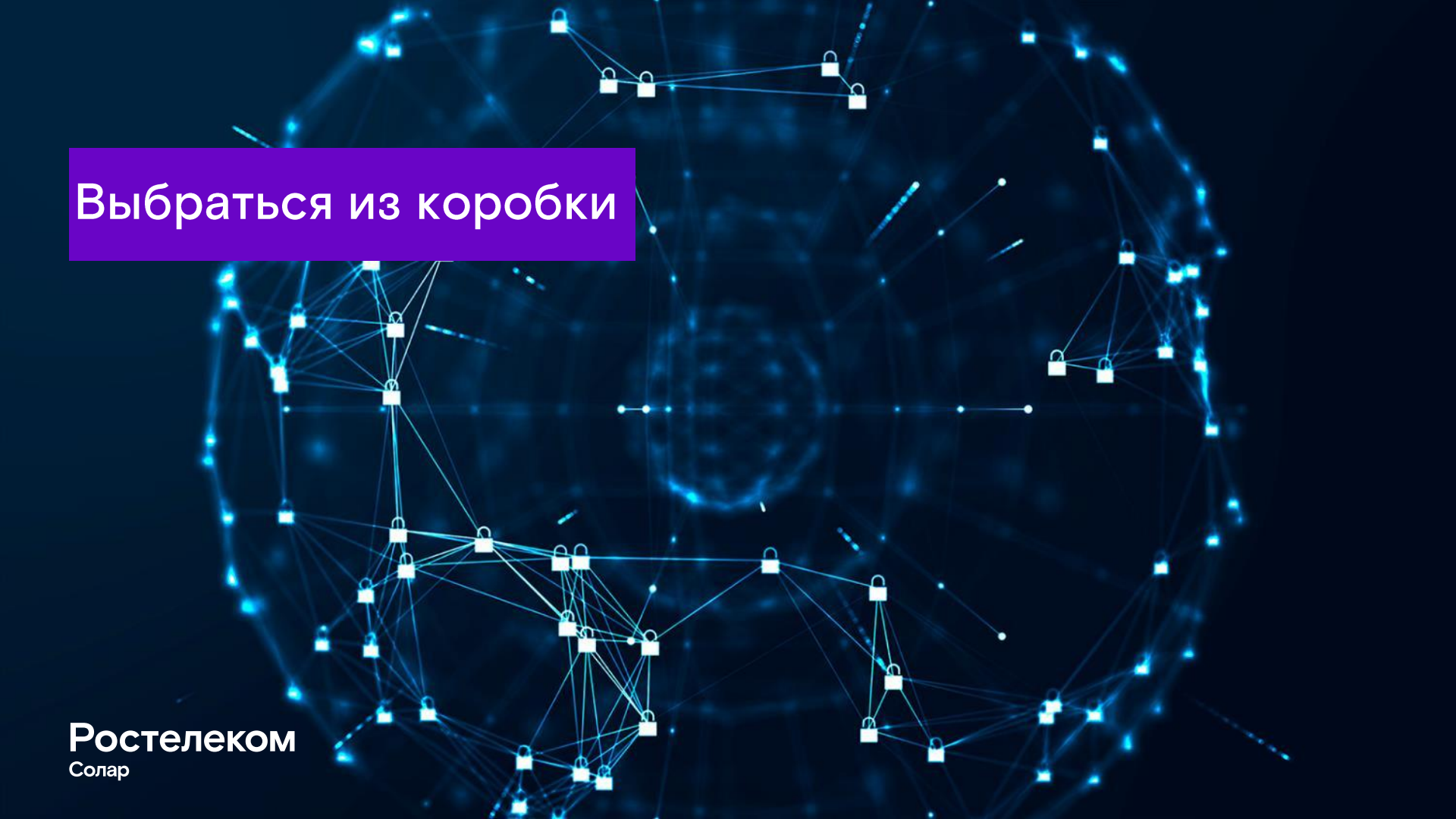
Классический метод пентеста



Проблемы классического метода

- Шумно
- Долго
- Проблема с установкой
- Множество ложных срабатываний
- Не стабильная работа эксплоитов
- Политика управления уязвимостями и обновлениями

Выбраться из коробки



Ростелеком
Солар

Ситуационная осведомленность на хосте

- Антивирусное ПО
  - AMSI
- Applocker
  - *Get-ChildItem -Path HKLM:\SOFTWARE\Policies\Microsoft\Windows\SrpV2\Exe*
  - *Get-AppLockerPolicy -Effective -Xml*
- PowerShell Constrained Language Mode
  - *$ExecutionContext.SessionState.LanguageMode*

Утилиты:

- SeatBelt (https://github.com/GhostPack/Seatbelt)
- HostRecon.ps1 (https://github.com/dafthack/HostRecon)

Сбор информации о сети

Удобный инструмент, на основе базы данных Neo4j, для сбора и анализа данных

- Визуализация данных
- Просмотр связей между объектами AD
- Построение векторов атак

Альтернативные варианты:

- ADExplorer
- PingCastle
- PowerVew

Пароли в Description

Простой и часто встречающийся вариант получения паролей в открытом виде

- *Get-DomainUser | Where-Object {$_.Description -ne $null}|Select-Object -Property samaccountname,description*
- *wmic /NAMESPACE:\\root\directory\ldap PATH ds_user GET ds_samaccountname,ds_description*
- Администраторы могут использовать другие поля

Пароли в GPO

- Group Policy Preferences (GPP)
- AutoLogon
- Reg файлы для настройки приложений
- Скрипты bat, vbs

Распыление Пароля

- Перебирается один пароль для всех пользователей
- Повторное использование одно пароля для разных учетных записей
  - user = adm_user
  - Сервисные учетные записи
  - Пароль по умолчанию принятый в компании
- Логин = Пароль
- Можно использовать после обнаружения пароля на других этапах

Kerberos

- С использованием Kerberos Password Spray генерируется событие ID 4771 (Kerberos pre-authentication failed) вместо 4625 (Logon Failure)

Общие файловые ресурсы

Некорректная установка прав доступа к файловым ресурсам могут привести к серьезным последствиям

- Файлы конфигураций
- Инструкции
- Текстовые записи
- Хранилища паролей (слабый master password)
- Резервные копии
- Почтовые архивы

Прожарка Kerberos

Kerberoasting

- SPN запись в атрибуте *ServicePrincipalName* доменной учетной записи
- Не изменяемые пароли для сервисных учетных записей

Aesrepoasting

- Флаг: «Do not require preauthentication»

Выполнение перебора пароля в offline

Ростелеком
Солар

MSSQL

- Доступ для авторизованных в домене пользователей
- Пароли в файлах конфигураций
- Пароли по умолчанию
- Логин = Пароль
- Хранимая процедура xp_cmdshell
- Связанные сервера
- Хранимые процедуры xp_dirtree и xp_fileexist -> NTLM Relay

Центр Сертификации AD

- SpecterOps провели исследование недостатков AD CS
  - *https://www.specterops.io/assets/resources/Certified_Pre-Owned.pdf*
- Некорректная настройка шаблона позволяет выпустить сертификат для любого пользователя домена
- Отсутствие подтверждения на выпуск сертификата

Что дальше?

Даже если предыдущие методы не дали привилегий доменного администратора они могут предоставить дополнительную информацию о сети или предоставить доступ к другим системам

- Боковое (горизонтальное движение)
- Неправильно настроенные ACL
  - GenericAll
  - GenericWrite
  - Force Change Password
- Делегирование Kerberos
  - Неограниченное делегирование
  - Ограниченное делегирование

Вопросы

Контакты

Центральный офис

125009 г. Москва,
Никитский переулок, 7с1

+7 (499) 755-07-70

info@rt-solar.ru

Ростелеком
Солар